ABSTRACT

Disclosed herein is an arithmetic logic unit over a finite field GF(2^m). Arithmetic logic units consistent with the present invention are disclosed as implemented using a division algorithm based on a binary greatest common divisor algorithm and a Most Significant Bit-first multiplication algorithm. The arithmetic logic unit can perform both a multiplication and a division using shared logic. Since the arithmetic logic unit has no limitations in the selection of an irreducible polynomial, and it is very regular and easily formed as a module, the arithmetic logic unit of the present invention has high expansibility and flexibility with respect to the size m of a field. Further, since the arithmetic logic unit of the present invention can perform a multiplication and a division using shared logic, it is very suitable to implement an encryption system for application products requiring a small size, such as smart cards or wireless communication devices.